NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

April 22, 2016

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Behavioral Science Technology, Inc. ("BST"), to inform you of a potential security incident that may have affected the personal information of one New Hampshire resident. BST is notifying affected individuals and outlining some steps they may take to help protect themselves.

On April 19, 2016, an unauthorized individual impersonating a BST executive contacted a BST employee by email requesting certain information for other BST employees. Before it was determined that the request was fraudulent, the BST employee provided a file that contained limited information about some of its employees, including first and last name, Social Security number, and 2015 compensation information. Fortunately, the file was password protected, and the password was not sent to the unauthorized individual. We currently have no evidence that any data in the spreadsheet was actually accessed or misused.

After learning of this incident, BST has conducted an investigation and has found no evidence that the unauthorized individual was able to gain access to any BST systems as a result of this incident or that any customer information, vendor information, or other employee information was impacted.

BST takes the privacy of personal information very seriously, and deeply regrets that this incident occurred. BST took steps to address and contain this incident promptly after it was discovered. Our employees in departments or functions with access to sensitive employee information will receive additional training concerning how to handle any requests for sensitive information and how to potentially recognize a "phishing scheme." BST will also work to raise awareness of all employees globally of these "phishing schemes" where fraudulent emails are

sent to BST employees requesting confidential information or action. In addition, BST has contacted law enforcement and will continue to cooperate in their investigation of this incident.

Affected individuals are being notified via a written letter, which includes an offer of complimentary identity protection and fraud resolution services. The notifications will begin mailing on or about April 22, 2016. A form copy of the notice being sent to the affected New Hampshire resident is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

Kristopher Kleiner

KCK
Enclosure

BST | now part of DEKRA Insight

[DATE]

[ADDRESS]

Dear [NAME],

Notice of Data Breach

We recently learned that Behavioral Science Technology, Inc. ("BST") was the victim of a data security incident that affects the personal information of some of our current and former employees. We are providing this notice as a precaution to inform potentially affected employees about the incident and to call your attention to some steps you can take to help protect yourselves. BST takes this matter very seriously, and we apologize for the frustration or concern this may cause you. We have arranged for impacted current and former employees to receive identity protection services for one year at no cost to you. Instructions for enrolling in these services can be found in the "What You Can Do" section below.

What Happened

On April 19, 2016, an unauthorized individual, impersonating a BST executive, contacted a BST employee to request certain information about BST employees. Before it was determined that the request was fraudulent, an electronic file was provided, which contained information about the affected employees. Fortunately, the file was password protected, and the password was not sent to the unauthorized individual. We currently have no evidence that any data in the file was actually accessed or misused.

What Information Was Involved

The file contained employee information including first and last name, Social Security number, and 2015 compensation information. Our investigation has found no evidence that this incident affected any of our network systems or that any other customer or vendor information was impacted.

What We Are Doing

We take the privacy and protection of your personal information very seriously at BST, and deeply regret that this incident occurred. We have taken steps to address the incident, including promptly alerting employees and working to investigate and remediate the situation. We have also contacted the Federal Bureau of Investigation and will cooperate fully with their investigation. Our employees in departments or functions with access to sensitive employee information will receive additional training concerning how to handle any requests for sensitive information and how to potentially recognize a "phishing scheme." BST will also work to raise awareness of all employees globally of these "phishing schemes" where fraudulent emails are sent to BST employees requesting confidential information or action.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft.

First, to help protect your identity, we are offering ***a year of complimentary identity protection services*** from Experian, a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about Experian's services, including enrollment instructions, please see the attached "Information about Identity Theft Protection" reference guide.

In addition to enrolling in the complimentary Experian services described above, we recommend that you ***carefully check your credit reports*** for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

1000 Town Center Drive • Suite 600 • Oxnard, CA 93036
Phone: (800) 548-5781 • Fax (805) 646-0328
www.BSTsolutions.com • email: bstusc@bstsolutions.com

Please also ***review the "Information about Identity Theft Protection" reference guide***, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

Finally, some of the information affected by this incident could be used to file a fraudulent tax return. As an additional precautionary measure, we recommend that you ***file a Form 14039 "Identity Theft Affidavit"*** with the IRS to help prevent someone from filing a fraudulent tax return in your name (either this year or in future tax years). For information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may also be similar resources and forms to file for individual states, so we recommend that you check directly with your state department of revenue for more information.

For More Information

If you have additional questions or if you would like to request an appointment to discuss your specific concerns by phone, you may contact us via email at securitysupport.dekrainsight.us@dekra.com. Again, we regret any inconvenience or concern caused by this incident.

Sincerely,

Dan McCleerey

Information about Identity Theft Protection

Identity Protection Services: Through Experian, BST is providing you with one year of complimentary identity protection services.

To enroll in the complimentary identity protection services:

- Visit **http://www.protectmyid.com/redeem** by **July 31, 2016** and use this personal activation code **[ACTIVATION CODE]**
  OR
- Enroll over the phone by calling **877.371.7902** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Provide the following **Engagement Number** as proof of eligibility: **XXXXXXX**.

Experian's identity protection services will include:

- A free copy of your **Experian credit report**.
- **Daily Bureau Credit Monitoring**: Alerts of key changes & suspicious activity found on your credit reports from all three credit bureaus (Experian, TransUnion, and Equifax).
- **$1 Million Identity Theft Insurance**[1]: Immediately covers certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Identity Theft Resolution & ProtectMyID ExtendCARE**: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate any incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - To offer added protection, you will receive ExtendCARE, which provides you with the same high-level of Fraud Resolution support indefinitely -- even after your ProtectMyID membership has expired.

Review Accounts and Credit Reports: We recommend that you regularly review credit and debit card statements and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant and continue to review your account statements and credit reports for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued your credit or debit card immediately. You should also promptly report

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. For more information please visit https://www.protectmyid.com/million-dollar-insurance.

any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. *You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.*

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213
Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872